Cybersecurity

Defending the New Battlefield

Steven J. Hutchison, Ph.D.

Cybersecurity is one of the most important challenges for our military today. Cyberspace is a new warfighting domain, joining the traditional air, land, sea and space domains—and cybersecurity considerations apply to almost all major defense acquisition programs.

Weapon systems and information technologies operate in an increasingly complex, networked, joint information environment, within which the threat has demonstrated itself to be remarkably agile, capable and persistent. To ensure programs are adequately prepared to deploy capabilities and support operations in the contested cyber domain, developmental testers must have robust, continuously improving methodologies and infrastructure to test and evaluate (T&E) our network-enabled military capabilities.

Hutchison *is the principal deputy for developmental test and evaluation in the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.*

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **DEC 2013**	2. REPORT TYPE	3. DATES COVERED **00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE **Cybersecurity: Defending the New Battlefield**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Acquisition University,Defense AT&L,9820 Belvoir Road,Fort Belvoir,VA,22060-5565**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**6**	

The Office of the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD[DT&E]) and Director, Test Resource Management Center (TRMC) has embarked on a course to improve the conduct of, and resources supporting, cybersecurity DT&E to set the conditions for improved production and deployment of enhanced capabilities to the warfighter. Dubbed "Shift Left" (see this author's article in the September–October issue of *Defense AT&L* magazine), the initiative fundamentally is about earlier identification of design issues and potential failure modes through mission-focused testing in the four key areas of performance, reliability, interoperability and cybersecurity.

Developmental testing always has had a focus on performance and reliability, although it generally has been characterized as "technical testing." Interoperability and cybersecurity testing, however, frequently are absent during DT&E since the certification processes permit programs to defer testing until after the decision to begin production. Technical focus and late testing cost programs in the long run. Hence, a Shift Left DT&E strategy adds mission context in all four key areas before production begins. A Shift Left strategy will help programs achieve Better Buying Power by avoiding the high costs and delays associated with problem discovery late in the life cycle. More important, a Shift Left strategy will help reduce the impact to our warfighters of fielding capabilities that do not satisfy user needs.

Military capabilities are vulnerable in the cyber domain. This of course is not a surprise, but the types of vulnerabilities and the ease with which they are uncovered is. Considerable data from testing cybersecurity in operational exercises show that fielded systems exhibit many common vulnerabilities. Clearly, programs should have found and corrected many of these vulnerabilities before fielding the system, which suggests the need to augment the certification and accreditation (C&A) process with robust cybersecurity DT&E to improve our ability to find and reduce system vulnerabilities. Therefore, to facilitate enhanced cybersecurity DT&E for acquisition programs, the office of the DASD(DT&E) and TRMC published Guidelines for Cybersecurity DT&E and operates the National Cyber Range (NCR) to

- Change how we think about and conduct cybersecurity testing.
- Help chief developmental testers and lead DT&E organizations develop and execute a robust cybersecurity DT&E strategy.
- Help acquisition decision makers understand cybersecurity risks.
- Improve resilience of network-enabled military capabilities.

The guidelines are available for download from the Acquisition Community Connection at https://acc.dau.mil/CommunityBrowser.aspx?id=22039.

Given our military dependence on network-enabled capabilities, the lack of a cybersecurity KPP is a major shortcoming with downstream effects in system development and DT&E, and ultimately places our warfighters at a disadvantage.

Background

DoD has long-standing processes for verifying the security of information systems. The first documented process appears to be the 1972 DoD Directive 5200.28 titled *Security Requirements for Automatic Data Processing (ADP) Systems,* reissued in 1988 as *Security Requirements for Automated Information Systems (AISs)*. These early directives also introduced the requirement for systems to have a Designated Approving Authority (DAA), and assigned responsibilities to the DAAs, many of which are still in use. For example, the 1988 directive stated: "The accreditation of an AIS shall be supported by a certification plan, a risk analysis of the AIS in its operational environment, an evaluation of the security safeguards and a certification report, all approved by the DAA." A companion DoD Manual (DoD 5200.28-M, January 1973) and DoD Computer Security Center Standard (CSC-STD-001-83, Aug. 15, 1983) titled *Trusted Computer System Evaluation Criteria*, provided guidelines for security testing. In December 1997, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD[C3I]) issued formal procedures for certification and accreditation (C&A) in DoD Instruction 5200.40, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*. The *DITSCAP* instruction defined security test and evaluation (ST&E) as "examination and analysis of the safeguards required to protect an IT system, as they have been applied in an operational environment, to determine the security posture of that system." The *DITSCAP* instruction also described the use of "penetration testing" during the validation phase as "strongly recommended to assess the system's ability to withstand intentional attempts to circumvent system security features by exploiting technical security vulnerabilities. Penetration testing may include insider and outsider penetration attempts based on common vulnerabilities for the technology being used."

Security testing remained under the purview of the DAA, however, which prompted an important distinction between DAA oversight of the C&A process and traditional T&E that resulted in a new director of operational test and evaluation policy in November 1999, to include operational testing of information assurance (IA) in the evaluation of system effectiveness and suitability. This guidance has remained in effect (with various updates) to the present.

Issuance of DoD Directive 8500.1, *Information Assurance,* in October 2002, canceled the 5200.28 directive, manual, and standard, although the DoD Instruction 8500.2, *Information Assurance Implementation*, in February 2003, continued DITSCAP as the applicable C&A process. In July 2006, the ASD for Networks and Information Integration (ASD[NII]) canceled DITSCAP, issued interim guidance, and then released DoD Instruction 8510.01 in November 2007, implementing the Defense Information Assurance Certification and Accreditation Process (DIACAP). The DIACAP process did not retain security test and evaluation. As this article was written, the next evolution of DoD information security policy was under way to replace DIACAP with the "risk management framework" (RMF). Among the notable changes, "cybersecurity" will replace "information assurance" and "Authorizing Official" will replace DAA.

The requirements system, or Joint Capabilities Integration and Development System (JCIDS), as described in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01H, does not address IA or cybersecurity, although earlier versions of JCIDS and the predecessor "requirements generation system" made limited references to IA. Acquisition programs have a set of "mandatory" key performance parameters (KPPs), including force protection, survivability, sustainment, Net-Ready (NR), training and energy. For a short time, IA was an element of the NR KPP. In November 2003, CJCSI 6212.01C introduced the NR KPP as a replacement for the interoperability KPP with IA as one of its four elements. However, satisfying this element of the NR KPP essentially was equivalent to completing DITSCAP or DIACAP. Therefore, in March 2012, CJCSI 6212.01F eliminated the IA element, noting that IA is the responsibility of a DAA. Today, cybersecurity appears only as a "potential attribute or consideration" of the survivability KPP. Given our military dependence on network-enabled capabilities, the lack of a cybersecurity KPP is a major shortcoming with downstream effects in system development and DT&E, and ultimately places our warfighters at a disadvantage.

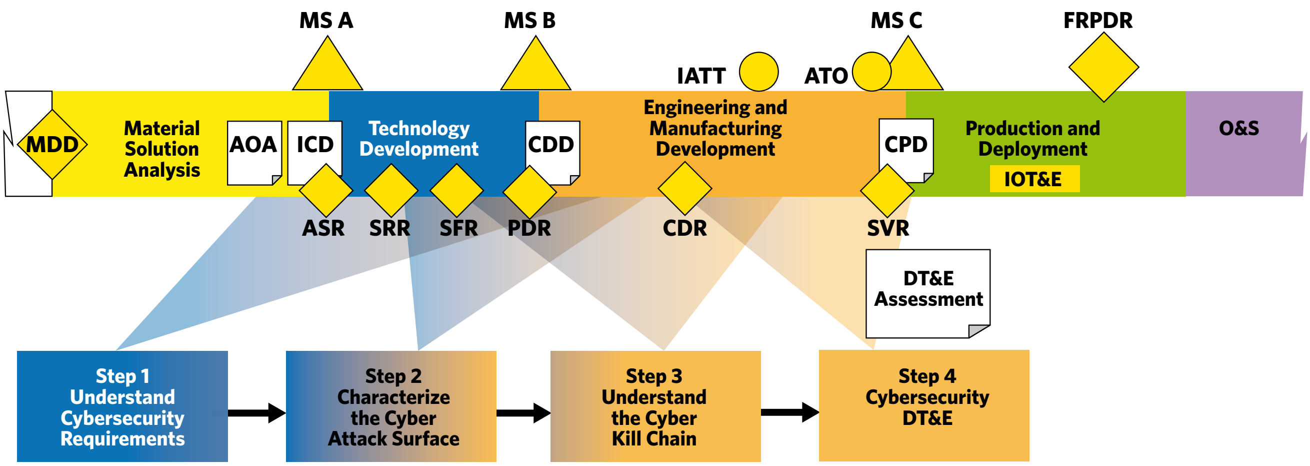
The parsing of IA/cybersecurity into "DAA space" has had, to some degree, the unintended consequence of decreasing its visibility in the acquisition, requirements and DT&E communities. Security test and evaluation never gained traction as DT&E practice since the DAA bases accreditation decisions upon the recommendation of a certifying authority, not a traditional test organization. The certifying authority rarely is included in the T&E working integrated process team (T&E WIPT), and the certification test strategy rarely is integrated into the T&E Master Plan (TEMP). For the DT&E community, the implications include insufficient numbers of, and training for, cybersecurity test professionals in the T&E career field; lack of well-defined cybersecurity metrics and evaluation framework; and uncertain capacity for supporting acquisition programs in cyber test facilities. With weak ties to the requirements and test community and a multitude of certifying authorities, the result is tremendous variability in implementing cybersecurity across the defense enterprise and, as field test data demonstrate, vulnerable systems that our cyber adversaries can exploit. The C&A process is necessary but not sufficient to ensure resilient systems in the field.

When combined with the C&A process, the Guidelines for Cybersecurity DT&E is a means to fill the test gap. The remainder of this article summarizes the guidelines.

Guidelines for Cybersecurity DT&E

The goal of cybersecurity DT&E is to improve the resilience of military capabilities in the presence of cyberattack. Cybersecurity DT&E extends beyond the foundation established

Figure 1. Cybersecurity DT&E process



through the C&A process to translate cybersecurity requirements, host environment, threat, and other considerations into meaningful tests designed to understand cybersecurity risks to the mission and improve resilience. Cybersecurity DT&E is a continuum of activities intended to improve production readiness at Milestone C. Figure 1 depicts cybersecurity DT&E in the acquisition life cycle. The steps may apply to different phases of the acquisition life cycle, depending upon the phasing of program engineering and production activities. Historically, TEMPs and associated test plans have not addressed adequately cybersecurity measures or resources such as cyber ranges. The chief developmental testers, lead DT&E organization and the certifying authority should seek opportunities to improve efficiency by integrating cybersecurity into other planned DT&E events. These guidelines should facilitate development and integration of cybersecurity into a comprehensive DT&E strategy that can be documented in the TEMP.

The cybersecurity DT&E process consists of four steps:

- Understand cybersecurity requirements.
- Characterize the cyberattack surface.
- Understand the cybersecurity kill chain.
- Cybersecurity DT&E.

In this model, requirements and testing bookend two important cybersecurity constructs: the *attack surface* and the *kill chain*. The attack surface generally describes the avenues by which a potential adversary may gain access to the system or data, and the kill chain generally describes what the adversary may be able to do if access is achieved—such as monitoring data exchanges, escalating privileges or embedding malicious software. Step 1 is a detailed analysis of documented requirements; these typically are *specified* tasks affecting system design. However, there are additional requirements that may not be documented formally. Step 2 considers the *implied* cybersecurity requirements necessary to reduce the overall attack surface. Step 3 identifies *essential* tasks necessary to reduce kill chain effects and ensure resilience in support of mission accomplishment in the contested cyberspace domain.

The concept of specified, implied, and essential tasks is analogous to the mission analysis in the military decision-making process (see Joint Pub 5.0). Step 4 executes cybersecurity DT&E to identify residual vulnerabilities so the developer and user can implement corrective actions before proceeding to production and deployment. A dedicated cybersecurity test event, such as testing in a cyber range, may be necessary to overcome limitations to testing on the live network.

The following paragraphs describe each step in the cybersecurity DT&E process.

Step 1: Understand Cybersecurity Requirements

This step is an analysis of system documentation to understand cybersecurity requirements. Chief developmental testers and lead DT&E organizations should examine thoroughly

> **For capabilities that operate in or exchange data through the cyberspace domain, developmental testers must have robust test methodologies and infrastructure to ensure these systems are prepared to support operations in the presence of cyber attack.**

system documents, including the relevant JCIDS capabilities document, program protection plan (PPP), information support plan (ISP), system threat assessment report (STAR), and others, to identify specified cybersecurity requirements. The purpose of the requirements review is to

- Identify cybersecurity requirements.
- Identify cyber threats to be emulated in test. For example, the January 2013 Defense Science Board report, "Resilient Military Systems and the Advanced Cyber Threat," describes the cyber threat in three levels of increasing sophistication divided into six tiers (http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf).
- Identify mission assurance category (MAC) and confidentiality level (CL) or risk category.
- Develop initial plan to integrate cybersecurity into overall DT&E strategy.
- Identify cybersecurity test organization(s), including:
  — DIACAP certifying authority/RMF security controls assessor.
  — **Blue Team**. During DT&E, the Blue Team may be a government organization or contractor equivalent. A Blue Team is a "group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and, in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cybersecurity

readiness posture. Oftentimes a Blue Team is employed by itself or prior to a Red Team employment to ensure that the customer's networks are as secure as possible before having the Red Team test the systems." (IA Glossary, NIST CNSSI 4009).
  - **Red Team**. During DT&E, the Red Team may be a National Security Agency (NSA)-certified government organization or contractor equivalent. A Red Team is "a group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise information assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment." (IA Glossary, NIST CNSSI 4009)
- Identify necessary cybersecurity DT&E resources.
  - Cyber range resources (e.g., NCR). During DT&E, the program may use a contractor-provided cyber range.
  - Modeling and simulation (M&S) tools for cybersecurity.

Step 2: Characterize the Cyber Attack Surface

The objective of Step 2 is to characterize the cyber attack surface to identify additional implied cybersecurity requirements. The attack surface may be defined as the system's exposure to reachable and exploitable vulnerabilities. System interfaces collectively contribute to the overall attack surface; in other words, any connection, data exchange, service, removable media, etc., may expose the system to potential threat access. Programs should not assume delivered support components (such as government-furnished equipment) are risk free; the system is only as secure as its weakest link. Chief developmental testers and lead DT&E organizations should accomplish the following during Step 2:

- Examine system architecture products (e.g., SV-1, SV-6) to identify interfacing systems, services, and data exchanges that may expose the system to potential threat exploits.
- Examine system Concept of Operations to understand roles and responsibilities of system operators, administrators, and the computer network defense service provider (CNDSP).
- Identify host environment provisions for system protection, monitoring, access control, system updates, etc.
- Analyze the attack surface to determine likely avenues of cyber attack.
- Determine system exposure to common vulnerabilities (examples in sidebar on Page 37).
- Evaluate early DIACAP/RMF and other security test artifacts.
- Identify test opportunities where representative systems and services will be available to conduct cybersecurity testing in a system-of-systems context (such as Joint Interoperability Test Command testing).
- Integrate DIACAP/RMF security controls assessment activities into unit testing, functional testing, etc.
- Refine the plan for integrating cybersecurity into DT&E activities.

Step 3: Understand the Cybersecurity Kill Chain

Step 3 focuses on identifying potential kill chain activities and closing vulnerabilities. Understanding how the cyber adversary may obtain access (the attack surface) is critical to determine potential actions the adversary may take. The cybersecurity kill chain is a sequence of actions used by a threat to execute a cyber attack. While there are variations of the kill chain, the typical stages include reconnoiter, weaponize, deliver, exploit, control, execute and maintain. Step 3 involves an analysis of potential kill chain activities to identify essential cybersecurity requirements necessary to improve resilience in the contested cyber domain. During this step, a Blue Team conducts cybersecurity testing during system integration tests and provides the program a vulnerability assessment of the system and its interfaces for corrective action. Chief developmental testers and lead DT&E organizations should accomplish the following during Step 3:

- For each attack surface vulnerability, determine likely kill chain activities.
  - Determine how the system is designed to respond to kill chain activities.
- Evaluate early DIACAP/RMF artifacts and identify vulnerabilities by DIACAP severity category. DoDI 8510.01 specifies severity categories as category (CAT) I, CAT II and CAT III.
  - CAT I weaknesses shall be corrected before an authorization to operate (ATO) is granted.
  - CAT II weaknesses shall be corrected or satisfactorily mitigated before an ATO can be granted.
  - CAT III weaknesses will not prevent an ATO from being granted if the DAA accepts the risk associated with the weaknesses.
- Using a Blue Team, perform a vulnerability assessment to determine the most likely threat exploits.
  - Scan systems and interfaces to determine potential vulnerabilities.
  - Include or emulate the CNDSP.
- Implement Blue Team-recommended corrective actions.
- Finalize the plan for Step 4 cybersecurity DT&E.

The results of Step 2 and Step 3 may help assign responsibility for corrective actions to the materiel developer, user, host environment or CNDSP.

Step 4: Cybersecurity DT&E

During Step 4, programs execute cybersecurity DT&E to confirm readiness for production. Step 4 evaluates system cybersecurity in a mission context, using realistic threat exploitation techniques. A Red Team performs cybersecurity testing, which may necessitate use of a cyber range to reduce the risk of collateral damage to live networks or authoritative data sources. Chief developmental testers and lead DT&E organizations should accomplish the following during Step 4:

Common Vulnerabilities

Password Practices
- Use of default passwords
- Poor user password practices
- Passwords stored on network devices without encryption or with weak encryption
- Use of keyboard pattern password

Privileged Access
- Standard user credentials with administrative privileges granted
- Use of shared administrator accounts
- Administrator accounts using identical UID/passwords across multiple server platforms
- Administrators using privileged accounts to access Internet Web servers

Access Control
- Use of unsecure ports and protocols (Port 80: HTTP)
- Use of prohibited ports and protocols
- Unsecure network services enabled on network devices and systems
- Anonymous File Transfer Protocol (FTP) allowed
- Lack of Access Control Lists (ACLs) implemented on border router

Computer Network Defense Service Provider (CNDSP) Monitoring and Operations
- Inadequate detection of insertion of removable media
- Host Based Security Services (HBSS) misconfiguration
- Unauthorized (rogue/malicious) devices installed on network not detected
- Use of physical intrusion devices not detected
- Unauthorized software installed on workstations not detected (HBSS)
- Misconfigured Intrusion Detection Systems (IDS)
- Data exfiltrations not detected

Workstations and Server Configurations
- Insecure configurations for hardware and software on mobile devices, laptops, workstations and servers (noncompliant remediation of known vulnerabilities)
- Unpatched server and workstation vulnerabilities (Buffer Overflow and Code Injection Vulnerabilities)
- Use of unauthorized software
- Unsecured SharePoint server
- Misconfigured services, servers and vulnerable drivers
- Network credentials, system configurations and network diagrams stored insecurely
- Web application vulnerable to Standard Query Language (SQL) injection attack (input validation vulnerability)
- Unauthorized data manipulation, due to weak data protections
- Operational information stored insecurely (no authentication or encryption used)
- Unsecured chat systems

Infrastructure
- No Wireless Intrusion Detection (WIDS) devices implemented
- Logging for infrastructure (network) devices not implemented
- Exploitation of two-way trust relationship between domains
- Physical security of critical components

- Evaluate final DIACAP/RMF artifacts:
  - — Have all CAT I and CAT II vulnerabilities been resolved?
  - — Is there a plan and schedule for remediating critical unresolved vulnerabilities before deploying the system?
  - — If mitigation or remediation efforts have been completed, have they been tested and included in the DT evaluation report?
- Using a Red Team, attempt to exploit the attack surface and execute cyber kill chain activities.
  - — Test in a cyber range if necessary. During DT&E, the program may use a contractor-provided Red Team and cyber range.
  - — Include or emulate the CNDSP.
  - — Include typical users if available.
  - — Identify exploitable threat vectors and vulnerabilities.
- Analyze results to determine impact to mission.
  - — Assess resilience to cyber attack effects.
- Recommend corrective actions to improve resilience.
  - — May include nonmateriel solutions, such as tactics, techniques, procedures (TTP) and recommendations to the CNDSP.

Cybersecurity DT&E may be an iterative process. Chief developmental testers and lead DT&E organizations should be cognizant of configuration changes, software and hardware updates and incremental development activities that deliver new features on a recurring basis that may necessitate follow-on analysis and cybersecurity DT&E.

Summary

Developmental test and evaluation helps programs set the conditions for improved production readiness and are essential to achieving the objectives of Better Buying Power and deploying improved capability to our warfighters in an effective and timely manner. For capabilities that operate in or exchange data through the cyberspace domain, developmental testers must have robust test methodologies and infrastructure to ensure these systems are prepared to support operations in the presence of cyber attack. The *Guidelines for Cybersecurity DT&E* and the National Cyber Range assist programs in developing and executing robust cybersecurity DT&E with the objective of improving the resilience of network-enabled military capabilities. By understanding the requirements, attack surface, and kill chain, developmental testers can identify the right set of metrics and design a robust cybersecurity DT&E strategy that will provide decision makers essential information and reduce the potential for problem discovery when it is too late to fix and a development problem becomes a warfighter problem.

The author may be contacted at **steven.j.hutchison.civ@mail.mil**.